



Intrinsically Assurable Mobile Ad-Hoc Networks

Proposer conference briefing

April 26, 2006

J Christopher Ramming
Program Manager, DARPA STO
James.Ramming@darpa.mil



Proposer conference purpose

- Describe solicitation
 - Don't try to read the fine print in my charts now. The charts will be posted on the web and are designed to be understood without my voiceover.
- Hear several gov't perspectives
- Provide teaming opportunities
- Answer questions

Objective: set the stage for a successful solicitation and subsequent program



CAVEATS

- I have no authority to bind the government
- In the event of any discrepancies between material here and material on FedBizOps, the FedBizOps material takes precedence



Background: Assurable Global Networking RFI & workshop

AGN RFI Questions

1. What should be the prioritized list of design criteria for a future Assurable Global Network that ultimately supports the DoD GIG?
2. What technology shortfall examples most clearly illustrate the need for a new architecture?
3. What concepts from the current Internet would need to evolve or change in order to support the proposed reprioritization?
4. What elements of the present-day Internet design can or should be retained in the future AGN?
5. To what extent does traditional "layering" impede progress toward the AGN? What might be the most appropriate abstractions and separations of concern in a future Internet? Consider both vertical layering and horizontal end-to-end considerations. Of particular interest are layerings that explicitly account for the relationship between network management, virtual private networks, and network control traffic.
6. There are many threats to information assurance other than network architecture, to include the inevitability of software bugs, the complexity of system configuration, the susceptibility of people to social engineering attacks, and the inevitability of human error. Are these orthogonal issues in information assurance or can network design help defend against these threats and if so how?
7. Are the needs of the DoD so different from users of the present Internet that a separate network architecture is needed, or can one architecture serve both needs?
8. What overall R&D roadmap (key milestones and general timeline) might lead to a deployable Assurable Global Network? Do not be unrealistically constrained by time, but consider rather what would be needed to achieve a fully featured result.
9. **What cornerstone high-payoff project or experiment should be executed in the short term to best create a foundation for a future AGN? Note: this is the most important question in the list. Ideally the answer follows logically from answers to the previous 8 questions.**

- RFI published mid-December
- Response deadline January 31
- Workshop Feb 22-23
- 52 position papers
- Many useful insights, covering both wired & wireless networks
- **See IAMANET web page for link to talks and papers**

The AGN RFI asked how to create an assurable network for the GIG (wired & MANET)

Internet Protocols are still vulnerable despite prior work

DARPA network defense focus

Global scale

Wireless

Tactical

92

94

96

98

2000

02

04

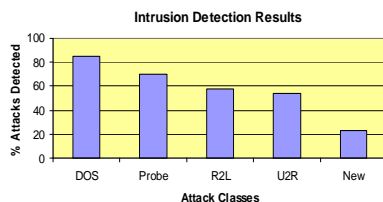
Today

- First prototype firewall
- Spawned industry market



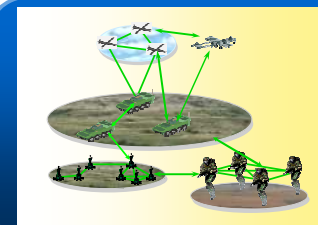
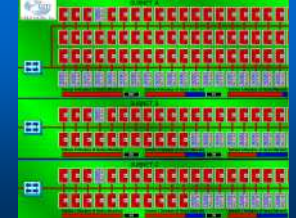
- Secure IP comms
- Commercial standards

- Distributed Denial of Service Solutions



- Significant advances in intrusion detection
- First objective measures
- Spurred nascent industry

- Enterprise system defense against zero-day attacks



- Mobile ad-hoc network defense

Internet-wide security protocols adopted by major back-bone providers

- S-BGP
- DNS Security

AGN insight: instead of fixing the Internet, we have been applying superficial bandages



Roots of vulnerability in Internet-based MANETs

Most
Important



Least
Important
(in fact,
ignored)

Original DARPA Internet design principles (in priority order)	
The Internet must support multiplexed utilization of existing interconnected networks.	
Internet communication must continue despite loss of networks or gateways.	
The Internet must support multiple types of communications service.	
The Internet architecture must accommodate a variety of networks.	
The Internet architecture must permit distributed management of its resources.	
The Internet architecture must be cost effective.	
The Internet architecture must permit host attachment with a low level of effort.	
The resources used in the internet architecture must be accountable.	

Threat model did not anticipate cyberattack, infiltration, exfiltration, or malicious control

Distributed management was partially achieved, but a cooperative basis for most protocols makes IP-based networks vulnerable to insider threat

Easy host attachment was made possible with a "permit-by-default" access policy (vs. a secure "deny-by-default" policy)

Without some form of accounting and accountability, malicious use of resources remains anonymous & untraceable

* Source: D. Clark, "The Design Philosophy of the DARPA Internet Protocols". Proc SIGCOMM 1988, Sept 1988.

Four key issues affecting information assurance were not addressed in the Internet design

“Assurable MANETs” must replace IP-based MANETs

DCAMANETS

- Distributed detection of malicious/infected/corrupted nodes from partial observations
- Dynamic reconfiguration and provisioning of services (e.g., GPS, tracking, common operational picture, threat information) or computational resources via coordinated autonomous operation of nodes
- Self-stabilizing behavior within bounded time for dynamic reconfiguration algorithms
- Distinguishing malicious behavior from legitimate behavior
- Identifying corrupted components and data to enable automatic reconstitution after attack
- Ensuring the cost of the response is much less than the cost of the event.

Defend a weak IP-based MANET

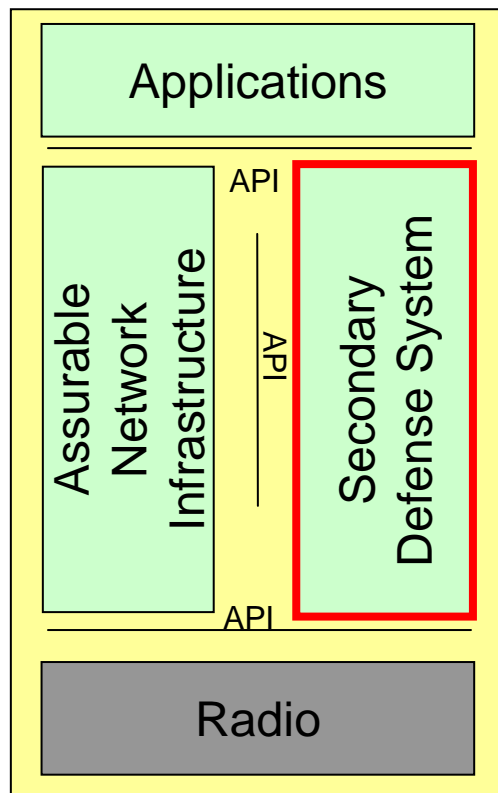
Assurable MANETs Phase 1

- Develop mechanisms for user accountability
 - Foundation of secure systems
- Reverse the Internet’s “permit by default” network access stance
 - Specify and enforce behavior contracts between applications and the network
- Develop a protocol stack addressing byzantine robustness
 - To handle (possibly multiple) colluding insiders
- Understand whether or not “trusted” tamper-proof hardware components are needed simplify the problem
 - If so, determine what minimal functions are needed

Make the MANET strong

IAMANET project: build a MANET based on assurable protocols instead of IP protocols

IAMANET System Model



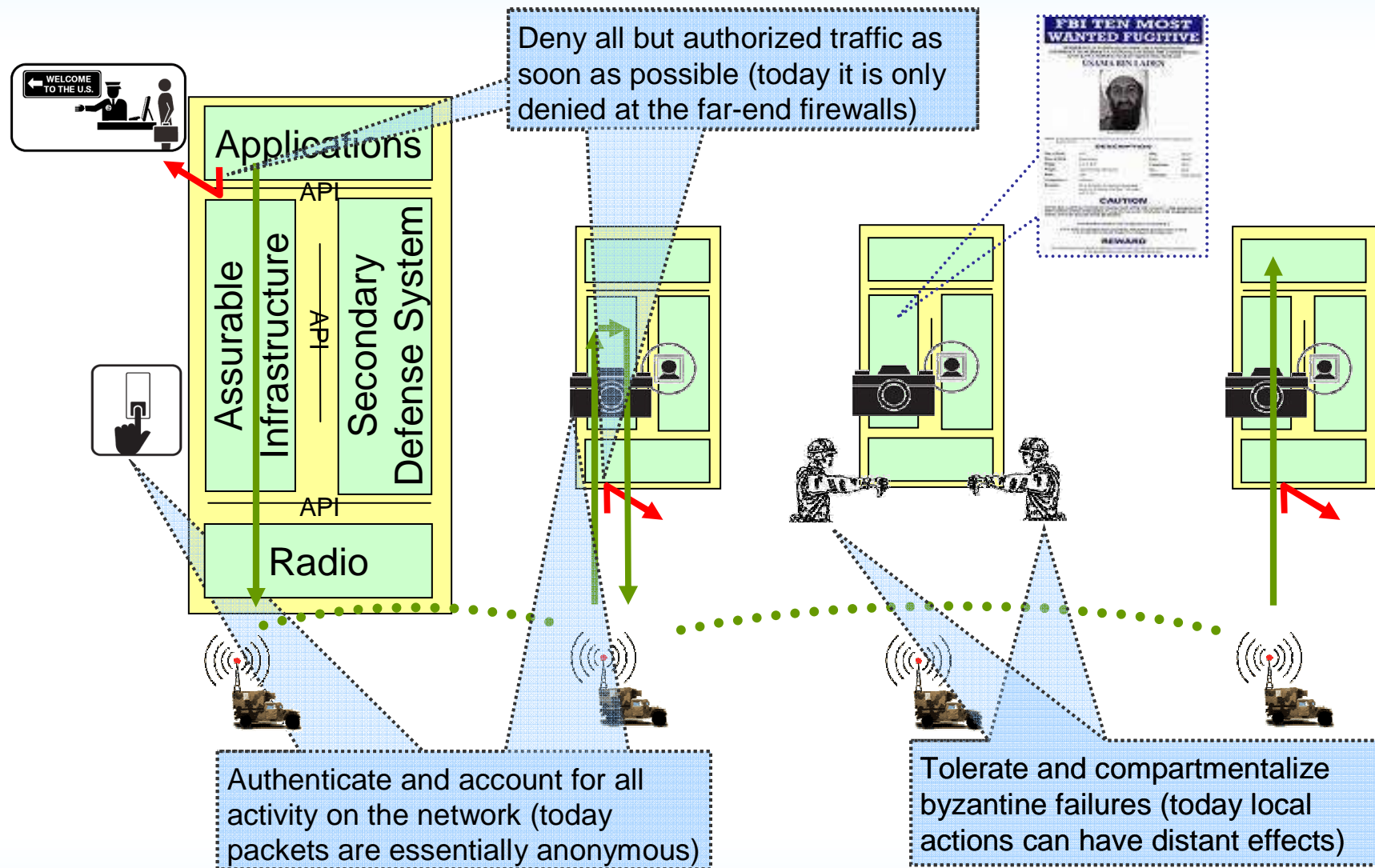
 **Unclassified subsystems**
(primary focus of Phase 1)

 **Radio (emulated or**
simulated in phase 1)

 **Optional collateral secret**
subsystem
(omitted for phase 1)

This system model offers a framework for describing programmatics

System model and key phase 1 security responses



Objective: minimize network subversion opportunities and consequences

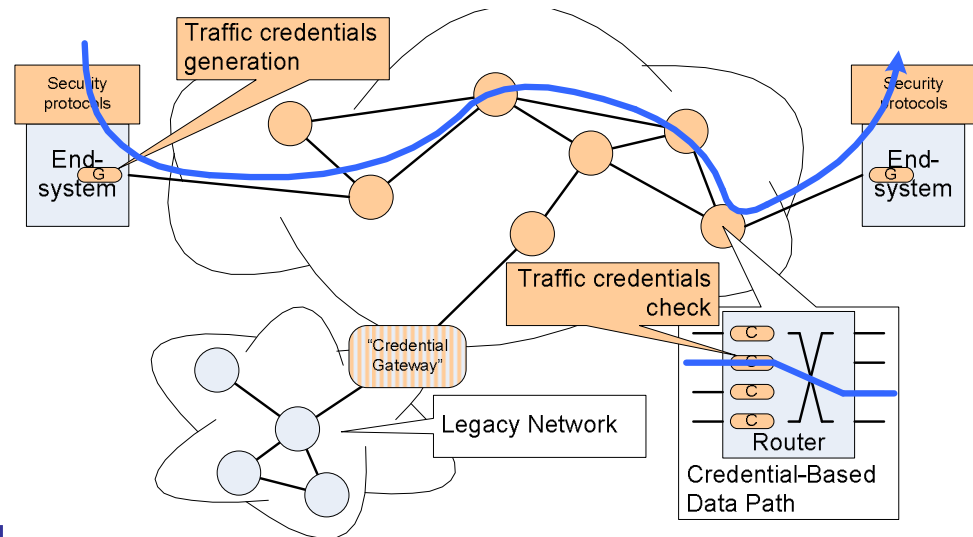
Way ahead: authenticate and account for all actions

Original DARPA Internet design principles (in priority order)

- The Internet must support multiplexed utilization of existing interconnected networks.
- Internet communication must continue despite loss of networks or gateways.
- The Internet must support multiple types of communications service.
- The Internet architecture must accommodate a variety of networks.
- The Internet architecture must permit distributed management of its resources.**
- The Internet architecture must be cost effective.
- The Internet architecture must permit host attachment with a low level of effort.

The resources used in the internet architecture must be accountable.

Without some form of accounting and accountability, malicious use of resources remains anonymous and untraceable



Benefits:

- Unauthorized users, attack traffic are tracked inside network, not just at end hosts
- Originator can be identified precisely
- Squelching can happen close to source
- Attackers can be traced back to source

Illustration: Authentication and credential checks throughout the network are one way to identify and hold users responsible for malicious or faulty activity.

Several [other] approaches are imaginable.

Accountability is needed for traceback, quarantine, and nonrepudiation

Way ahead: deny by default any unauthorized activity

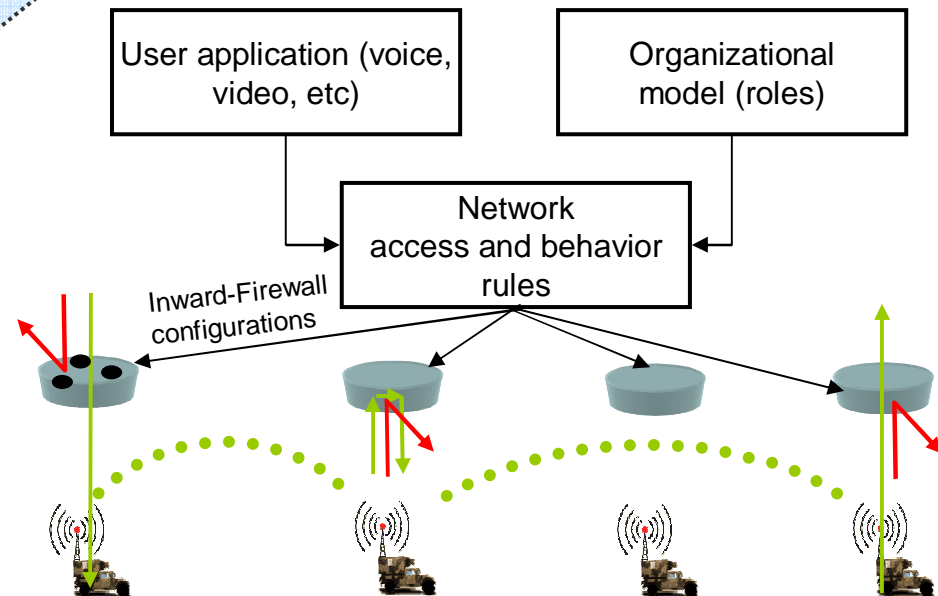
Original DARPA Internet design principles (in priority order)

- The Internet must support multiplexed utilization of existing interconnected networks.
- Internet communication must continue despite loss of networks or gateways.
- The Internet must support multiple types of communications service.
- The Internet architecture must accommodate a variety of networks.
- The Internet architecture must permit distributed management of its resources.
- The Internet architecture must be cost effective.

The Internet architecture must permit host attachment with a low level of effort.

The resources used in the internet architecture must be accountable.

Easy host attachment was made possible with a “permit-by-default” access policy (vs. a secure “deny-by-default” policy)



Benefits:

- New threats/actions are often denied a priori
- Prevents denial-of-service attacks
- “Probing” is severely limited and easily curtailed
- Anomaly detection is simplified due to narrower scope of permitted actions

Illustration: program behavior specifications could be used to configure generalized, distributed inward-facing firewalls.

Several [other] approaches for enforcing a network/application contract are imaginable.

Unauthorized traffic must be kept off “the network” to simplify defense

Way ahead: compartmentalize byzantine* failures

Original DARPA Internet design principles (in priority order)

The Internet must support multiplexed utilization of existing interconnected networks.

Internet communication must continue despite loss of networks or gateways.

The Internet must support multiple types of communications service.

The Internet architecture must accommodate a variety of networks.

The Internet architecture must permit distributed management of its resources.

The Internet architecture must be cost effective.

The Internet architecture must permit host attachment with a low level of effort.

The resources used in the internet architecture must be accountable.

*** Definition:** byzantine failures (as opposed to halting failures) involve continued operation with unexpected and possibly malicious behavior

Benefits:

- Tolerates insider threat
- Prevent specific attacks (sybil, black hole, rushing)

Threat model did not anticipate cyberattack, infiltration, exfiltration, or malicious control

Distributed management was partially achieved, but a cooperative basis for most protocols makes IP-based networks vulnerable to insider threat

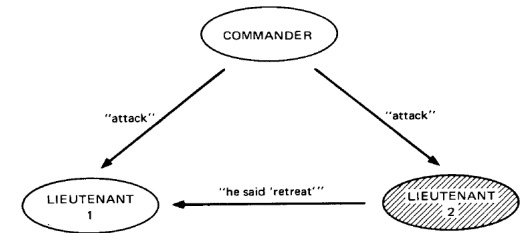


Fig. 1. Lieutenant 2 a traitor.

Original illustration of Lamport's oral agreement algorithms. Agreement can be obtained as long as less than 1/3 of participants are traitors.

Byzantine agreement framework				
	Oral agreement	Signed agreement	Optimistically terminating consensus	BAR
Component behavior	n	n	n	n
		n/a	f	r
				a
	m	m	m	m
Requirement	$n \geq 3m + 1$	$n \geq 2$	Various formulations	???
Worst case # rounds	$m + 1$	$m + 1$	Depends on actual numbers	???

Properties of several agreement frameworks that could be a basis for new MANET protocols.

Several [other] approaches are imaginable.

Protocols with byzantine robustness are needed to survive malicious insiders

Research question: role of tamperproof hardware

Original DARPA Internet design principles (in priority order)

The Internet must support multiplexed utilization of existing interconnected networks.

Internet communication must continue despite loss of networks or gateways.

The Internet must support multiple types of communications service.

The Internet architecture must accommodate a variety of networks.

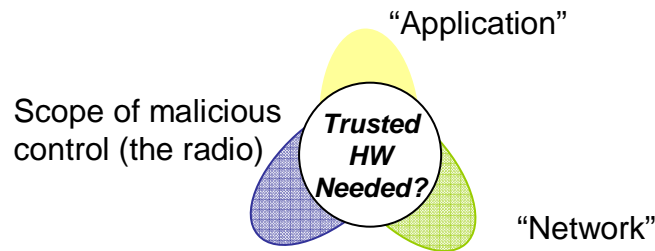
The Internet architecture must permit distributed management of its resources.

The Internet architecture must be cost effective.

The Internet architecture must permit host attachment with a low level of effort.

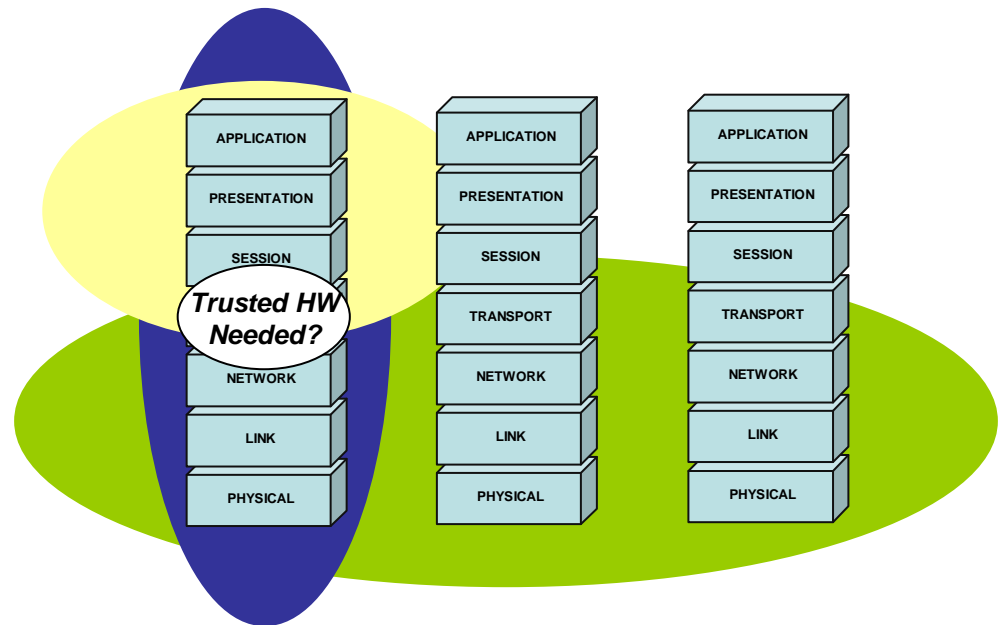
The resources used in the internet architecture must be accountable.

A cold-war era threat model did not anticipate cyberattack, infiltration, exfiltration, or malicious control



Benefits:

- May prevent egregiously noncompliant behavior
- May simplify defensive system



Because the radio can be captured, and “contains” part of the network we may need tamper-proof hardware in the radio.

Open question: what minimal functions at the intersection Of the network and the application must be implemented in a tamper-proof trusted computing hardware?

Some tamperproof hardware may be needed to implement an assurable MANET



Non-exhaustive list of cyberattack possibilities

Attack Type	Description	Examples
Network protocol	Exploit characteristics of network protocols to degrade performance	Jellyfish attack, Blackhole attack
Routing	Exploit characteristics of routing protocols to degrade performance	Spoofing, altering, or replaying routing info
Data integrity	Modify data or data characteristics to degrade performance	Message injection or replay; selective forwarding, reordering, or corruption of data
[D]DoS	Deny legitimate users access to resources and services	Flooding; resource exhaustion
Authentication and identity	Exploit the identity and/or authentication system to degrade performance	Credential compromise; masquerading; spoofing; Sybil attack
Sinkhole	Cause traffic to be routed through a compromised node (to facilitate or amplify other attacks)	Rushing attack
Topology obfuscation	Obscure true network topology to degrade performance	Wormhole attack; exchange of false routing info; ACK spoofing
Cooperative	Use multiple nodes to amplify or enable attacks	Multiple nodes collude to win a distributed vote

Vulnerabilities enable attacks that are one way to affect availability, integrity, & other factors

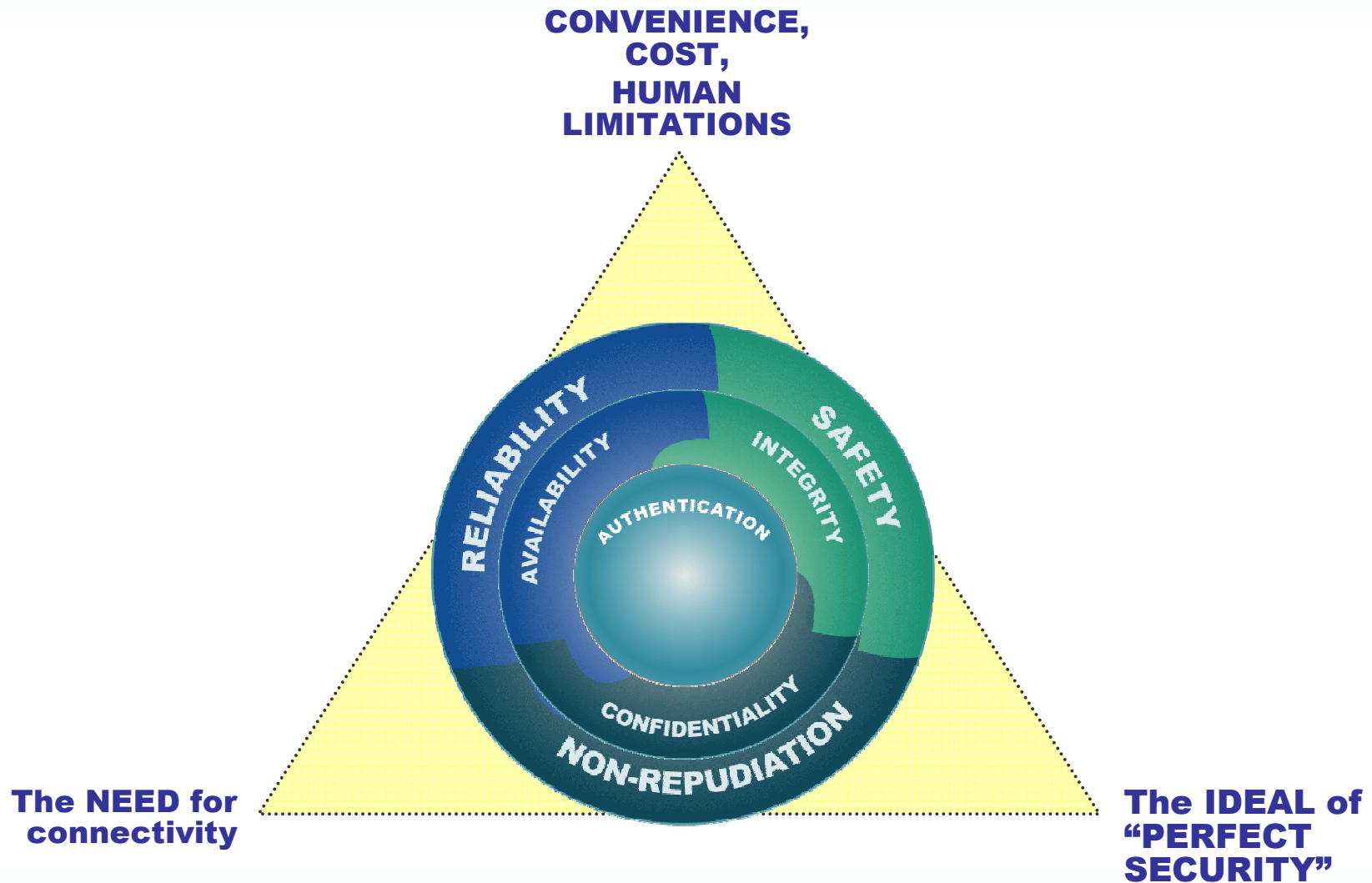


Worm Characteristics

Characteristic	Examples
Targeting technique	Scanning (random, sequential, permutation, meta-server); pre-generated target lists (local or remote); host-resident data; passive inferencing; exploitation of MAC layer information
Targeting breadth	Target specific hosts/roles; achieve max infection rate
Propagation vector	Vulnerabilities in applications, services, routing layer, OS kernel; misconfigurations; privilege escalation; use of multiple propagation vectors
Propagation channel	Unicast; multicast; broadcast
Propagation speed	Slow/stealthy; fast; flash (efficient tree, multicast, etc.)
Transfer technique	Self-carried; second-channel; embedded
Activation	Immediate; triggered (human or event); scheduled
Counterdefensive techniques	Metamorphism; polymorphism; obfuscation; persistence

Worms augment the scope of vulnerability impact

Aside: some tradeoffs in information assurance



Ease of use, security, and connectivity must be carefully balanced



Aside: configuration complexity as a vulnerability

- **65% of attacks exploit misconfigured systems.**
 - British Telecom/Gartner Group.
 - http://www.btglobalservices.com/business/global/en/products/docs/28154_219475secur_bro_single.pdf
- **Human error accounts for 48% of wide area network outages**
 - Yankee Group 2002
- **...operator error is the largest cause of failures...and largest contributor to time to repair ...** in two of the three (surveyed) ISPs.....configuration errors are the largest category of operator errors. – David Oppenheimer, Archana Ganapathi, David A. Patterson. *Why Internet Services Fail and What Can Be Done About These? Proceedings of 4th Usenix Symposium on Internet Technologies and Systems (USITS '03)*, 2003.
 - <http://roc.cs.berkeley.edu/papers/usits03.pdf>
- **45% WAN operations cost attributed to component configuration**
 - Yankee Group, 1998
- **Although setup (of the trusted computing base) is much simpler than code, it is still complicated, it is usually done by less skilled people,** and while code is written once, setup is different for every installation. **So we should expect that it's usually wrong, and many studies confirm this expectation.** – Butler Lampson, *Computer Security In the Real World. Proceedings of Annual Computer Security Applications Conference*, 2000.
 - <http://research.microsoft.com/lampson/64-SecurityInRealWorld/Acrobat.pdf>
- **Consider this:the complexity [of computer systems] is growing beyond human ability to manage it....the overlapping connections, dependencies, and interacting applications call for administrative decision-making and responses faster than any human can deliver.** Pinpointing root causes of failures becomes more difficult. –Paul Horn, Senior VP, IBM Research. *Autonomic Computing: IBM's Perspective on the State of Information Technology*.
 - http://www.research.ibm.com/autonomic/manifesto/autonomic_computing.pdf

Ease and simplicity of proper configuration are an important aspect of assurability



End-of-program goals / metrics

OBJECTIVES:		
Metric	Threshold for all phases	Notes
Cyberattack containment	Red team with full knowledge of network and defensive system cannot create attack that negatively affects any 2-hop neighbor of a subverted node	<ul style="list-style-type: none"> •This metric implicitly includes preventing worms from propagating beyond the source node where they could affect more distant neighbors. •The metric contains implicit man-year limits on red team activity based on funding (no security is perfect) •In Phase 1, the performers <u>are not</u> responsible for mitigating lifecycle attacks •In Phase 2, the performers <u>are</u> responsible for mitigating lifecycle attacks
Data exfiltration	Red team with full knowledge of network and defensive system cannot exfiltrate operational information from the MANET	<ul style="list-style-type: none"> •Exfiltration (of location info, for instance) is an important threat •Stresses authorization, credentialing, & accountability •In Phase 1, the performers <u>are not</u> responsible for mitigating lifecycle attacks •In Phase 2, the performers <u>are</u> responsible for mitigating lifecycle attacks
SUBJECT TO:		
Ability to support multiple application types	<ul style="list-style-type: none"> •Unicast and Multicast data (real-time voice/video, reliable files) •Total exchange applications (situation awareness) •File transfer (map download) •Group and peer-to-peer applications (chat) •Urgent or time-sensitive messages (call for fire, real-time control) 	<ul style="list-style-type: none"> •Consider QoS, jitter, latency constraints
MANET performance while not under attack	Performer MANET must be capable of supporting the same representative traffic load as a government-defined baseline “non-assurable” MANET	<ul style="list-style-type: none"> •Both networks to use equivalent hardware resources •Sample testbed, baseline network, and scenarios to be provided by the Government •72 node MANET •Baseline protocols: 802.11 + OLSR + UDP/IP + diffserv.
Ability to multiplex data over multiple network types	Performer protocols can support traffic loads that cross network boundaries, to include at least one wired network	<ul style="list-style-type: none"> •Tested with reachback traffic load

No security is perfect, but these metrics should be achievable against a funded red team



Phase tasking

Phase 1:

- Performers
 - Research, document, and prototype an end-to-end assurable MANET architecture excluding secondary defensive system
 - Self-test and evaluation against program metrics
 - Support installation at red-team facility and host a red-team analysis on-site
 - Support red-team's analysis against program metrics
- Government
 - Provide demonstration suite of baseline protocols, proxy applications, mobility models, and representative traffic loads
- Red team
 - Analysis and attacks

Phase 2 and beyond:

- Performers
 - Research, prototype, integrate, evaluate, and field test with secondary defensive system
- Government
 - GFE radio hardware
- Red team
 - Attacks and analysis

Color key:
Unclassified (black)
Likely classified (red)

Phase 1: An assurable network

Phase 2: An assured network

Red team test & evaluation

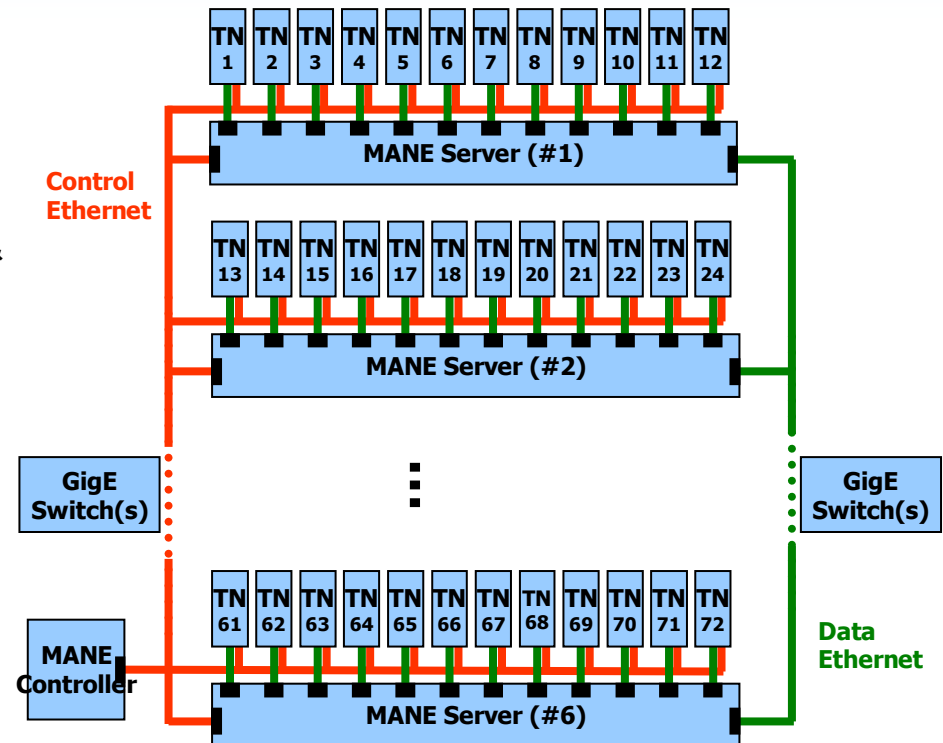
Analysis-based adversarial red-teaming, possibly coupled with vulnerability demonstrations

Phase 1:

- Red team has full prior access to performer design & implementation
- Red team is permitted to assume control of two or more nodes (to test byzantine robustness)
 - Exception: designated “tamperproof hardware” functions
- Red team may build arbitrary attack applications but changes to the network stack and applications are limited to byzantine errors
 - Not permitted to insert buffer overflows etc until phase 2

Phase 2:

- All of the above freedoms without limitation plus:
- Red team is permitted to insert artificial software vulnerabilities to simulate typical buggy code and lifecycle attacks
 - Exception: designated “tamperproof hardware” functions
- Phase 2 red team techniques & report may be classified



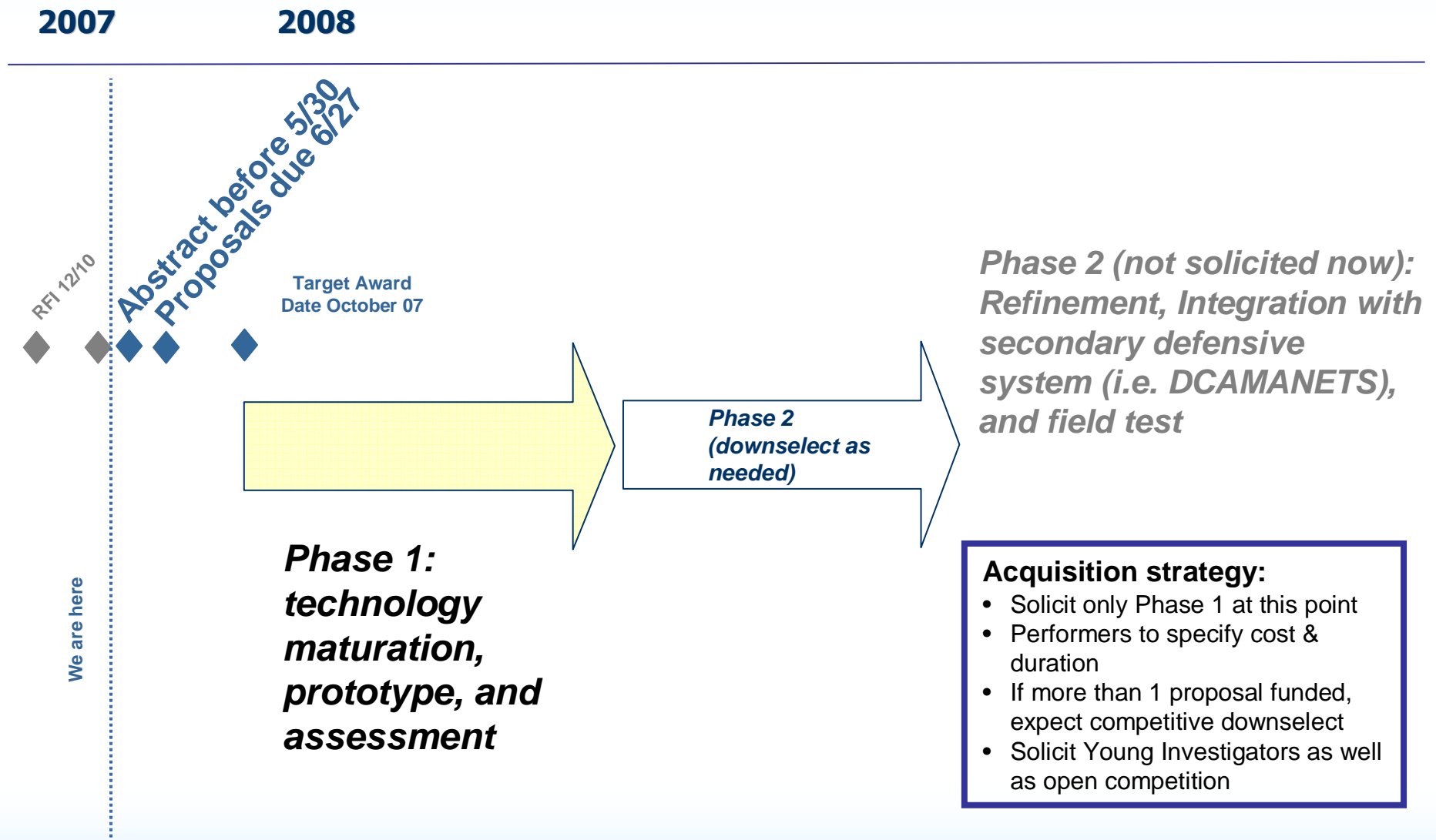
TN = Test Node (Kontron C6000 and Dell D800)
MANE Server (Dell PowerEdge 2850)

Performers must use a testbed of some sort to show basic networking performance and must self-analyze the threats and vulnerabilities of the system

Ideally, even full internal knowledge of performer systems should not help a red team



Assurable MANETs Program Schedule



Only phase 1 is solicited at this time; performers to specify cost & duration



BAA/RA Evaluation Criteria

- TECHNICAL AND ARCHITECTURAL APPROACH
- ASSURABILITY OF THE PROPOSED SOLUTION
- MANAGEMENT APPROACH AND QUALIFICATIONS OF THE KEY INDIVIDUALS
- CONSTRUCTIVE PLAN / RESEARCH AGENDA
REALISM
- POTENTIAL CONTRIBUTION AND RELEVANCE TO THE DARPA MISSION
- COST AND SCHEDULE REASONABLENESS AND REALISM

Criteria are in order of importance



Early-career investigator research announcement

- An "Early-Career Investigator" is defined to be a researcher who meets all of the following criteria:
 - Holds a tenure-track faculty position at a U.S. institution of higher learning;
 - Is not tenured as of the date this proposal will be due
 - Was awarded a PhD no earlier than January 1, 1998; and
 - Received a first appointment as faculty member no earlier than January 1, 1998.
- RA is open to teams of grant institutions in which the principals meet the Early-Career Investigator definition
- Proposals with excessive or gratuitous industry involvement will be considered noncompliant.

Expectations of the RA proposals are very high. Evaluation is identical to the BAA.



Security considerations

- Phase 1 planned to be unclassified
- Aspects of subsequent phases will be classified
- Proposer must intend to participate in subsequent phases
- Proposers must outline the means whereby they will be able to continue work in subsequent phases
 - Proposals not meeting this standard will be considered non-compliant
- These provisions do not preclude the possibility of university-based research in Phase 1!

Onus is on proposers to find a workable solution

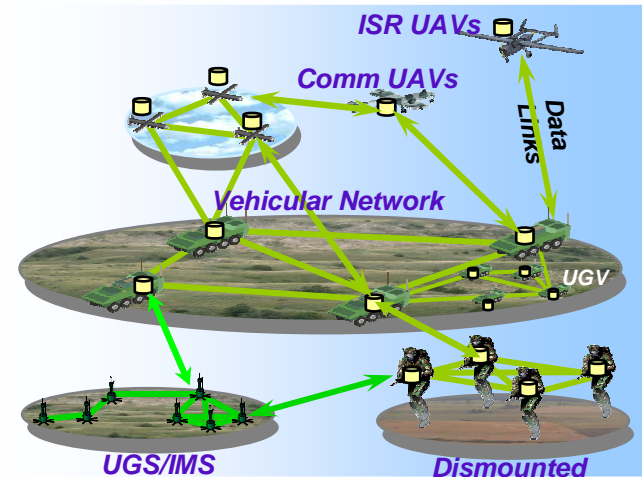
Summary: Assurable MANETs program

Status quo

MANETs based on Internet protocols are inherently vulnerable to malicious hosts, possibly leading to total subversion and/or system shutdown

Metrics

Contain attacks and prevent exfiltration, subject to acceptable performance for multiple applications types and support for multiplexing across networks



System responses

Ideal: an Assurable MANET

- **Integrity:** network does not collapse due to cyberattack or presence of faulty or malicious components
- **Availability:** data can traverse network despite presence of faulty or malicious components
- **Reliability:** infected processes and nodes are reconstituted to ensure availability over mission duration
- **Confidentiality:** malicious data exfiltration is denied
- **Safety:** network only engages in activities specified by the protocols
- **Non-repudiation:** users cannot repudiate actions taken on the network

- Authenticate and account for actions taken throughout the network to enable traceback and nonrepudiation
- Deny by default any unauthorized activity
- Tolerate and compartmentalize byzantine failures (i.e. the presence of malicious or faulty components)
- Detect, trace back, and quarantine harmful activity
- Dynamically reconfigure, re-provision, and reconstitute network to maximize throughput while under attack

Phase 1

DCAMANETS

Phase 2

Objective: minimize network subversion opportunities and consequences



Questions?

- Ask questions on 3x5 cards (one question per card)
- Q&A panel this afternoon
- Additional questions to iamanet-solicitation@darpa.mil
- Please check the IAMANET website for answers and Q&A updates during the proposal preparation process

<http://www.darpa.mil/sto/solicitations/IAMANET/index.htm>